EXHIBIT A

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

BRADY COHEN, *individually and on behalf of all other similarly situated*, Plaintiffs, -against- CASPER SLEEP INC. and NAVISTONE, INC., Defendants.	17cv9325
BRADY COHEN, *individually and on behalf of all others similarly situated*, Plaintiffs, -against- NAVISTONE, INC. and CHARLES TYRWHITT, INC., Defendants.	17cv9389
BRADY COHEN, *individually and on behalf of all others similarly situated*, Plaintiffs, -against- NEW MOOSEJAW, LLC and NAVISTONE, INC., Defendants.	17cv9391 OPINION & ORDER

WILLIAM H. PAULEY III, Senior United States District Judge:

Defendants Casper Sleep Inc. ("Casper"), Charles Tyrwhitt, Inc. ("Tyrwhitt"), New Moosejaw, LLC ("Moosejaw") (collectively, the "Retailers"), and NaviStone, Inc. ("NaviStone") move to dismiss this putative class action alleging claims under the Electronic Communications Privacy Act ("ECPA"), Stored Communications Act ("SCA"), and New York General Business Law ("GBL").[1] For the following reasons, Defendants' motions are granted.

BACKGROUND

The allegations of the Complaints are presumed true on this motion. Brady Cohen seeks to represent a nationwide class of similarly situated website visitors whose electronic communications—such as mouse clicks and keystrokes—were intercepted by Defendants. (First Am. Class Action Compl., Casper ECF No. 28 ("Casper Compl."), ¶¶ 1–3, 53.) He also seeks to represent a New York subclass. (Casper Compl. ¶ 53.)

NaviStone is a marketing company and data broker that offers computer code (the "Code") to e-commerce retailers to help them identify who visits their websites. Specifically, the Code allows e-commerce retailers to scan website visitors' computers for information that can be used for de-anonymization, as well as to observe their keystrokes, mouse clicks, and communications with the e-commerce retailers' websites. (Casper Compl. ¶ 1.) Hundreds of online retailers entered into voluntary partnerships with NaviStone to insert the Code into their websites. (Casper Compl. ¶¶ 11, 15.) Casper (a mattress manufacturer and retailer), Tyrwhitt (a men's clothing company), and Moosejaw (an active outdoor retailer) were three such retailers who embedded the Code into their websites. Defendants hid the embedded Code from

[1] Cohen filed three separate lawsuits: (1) against Casper and NaviStone (17cv9325), (2) against Tyrwhitt and NaviStone (17cv9389), and (3) against Moosejaw and NaviStone (17cv9391). This Opinion and Order dismisses each lawsuit and will be filed separately on each docket. The three complaints contain largely parallel allegations. For ease of reference, this Court cites primarily to the Casper Complaint.

consumers using "dummy domains," which cannot easily be traced back to NaviStone. (Casper Compl. ¶ 17.)

Cohen claims the Code functions as a "wiretap." Specifically, he alleges the Code serves as a "back door" permitting NaviStone to access the Retailers' websites and intercept web visitors' electronic communications. (Casper Compl. ¶ 12.) Thus, as soon as web users visit the Retailers' websites, the Code "spies" on those visitors in real time as they browse, capturing their keystrokes and mouse clicks and contemporaneously sending that information to NaviStone. (Casper Compl. ¶ 13.) The Code also reports every page visited by users and any items added to their carts, (Casper Compl. ¶ 33), as well as any information provided on data forms, even if not submitted (Casper Compl. ¶ 34). As such, NaviStone acquires visitors' IP addresses and other Personally Identifiable Information ("PII"). Cohen further alleges that the Code scans visitors' devices for data files containing PII. (Casper Compl. ¶ 13.) During such a scan, the Code searches for "tracking files" employed by other websites similar to NaviStone. (Casper Compl. ¶ 32.)

According to the Complaint, NaviStone maintains a database containing profiles of U.S. consumers, including their names and addresses. When users browse websites containing the Code, NaviStone "matches," or compares, elements of the intercepted data to its database. When there is a match, NaviStone de-anonymizes website users and updates its database with the users' current browsing activities and PII. (Casper Compl. ¶ 14.)

Cohen further alleges that Casper violated its privacy policy ("Privacy Policy"). Specifically, Cohen claims that Casper's Privacy Policy is misleading because it fails to disclose that certain information is intercepted by NaviStone. (Casper Compl. ¶¶ 41, 44.) Cohen does not assert such a claim against Moosejaw or Tyrwhitt.

Finally, Cohen alleges that the Retailers embedded the Code on their websites and that the Code scanned his Android device and intercepted his electronic communications for de-anonymization. (Casper Compl. ¶¶ 1–2; First Am. Class Action Compl., Moosejaw ECF No. 29 ("Moosejaw Compl.") ¶¶ 1–2; First Am. Class Action Compl., Tyrwhitt ECF No. 26 ("Tyrwhitt Compl.") ¶¶ 1–2.) Cohen accessed each Retailer's website and neither knew nor consented to the interception of his data. (Casper Compl. ¶¶ 2, 4.) As such, Cohen asserts eight claims: (1) five claims under the Electronic Communications Privacy Act, (2) one claim under the Stored Communications Act, and (3) two claims under the New York General Business Law.

DISCUSSION

I. Standard

On a motion to dismiss for failure to state a claim under Federal Rule of Civil Procedure 12(b)(6), a court must accept as true all well-pleaded facts and draw all reasonable inferences in the light most favorable to the non-moving party. Kassner v. 2nd Ave. Delicatessen Inc., 496 F.3d 229, 237 (2d Cir. 2007). "To survive a motion to dismiss, the plaintiff's pleading must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (citation and quotation marks omitted). Moreover, a claim must rest on "factual allegations sufficient to raise a right to relief above the speculative level." Bell Atl. Corp. v. Twombly, 550 U.S. 544, 555 (2007). As such, a pleading that offers "labels and conclusions" or a "formulaic recitation of the elements of a cause of action" fails to state a claim. Iqbal, 556 U.S. at 678 (citation omitted).

II. Electronic Communications Privacy Act Claims

Cohen brings claims under 18 U.S.C. § 2511 (the Wiretap Act) and 18 U.S.C. § 2512. Each is discussed in turn.

A. Section 2511 Claims

Under 18 U.S.C. § 2511(1), "[a]ny person who--

> (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication; . . .
>
> (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; [or]
>
> (d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; . . .
>
> shall be subject to suit as provided in subsection (5).

Cohen brings claims under subsections (a), (c), and (d), all of which, in some form, require intentional action and an interception of an electronic communication in violation of the subsection. As such, these claims may be analyzed together.

As a threshold matter, Cohen's Wiretap Act claims falter because § 2511 is a one-party consent statute. Section 2511 states that "[i]t shall not be unlawful under this chapter for a person . . . to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception . . . ." 18 U.S.C. § 2511(2)(d). It is clear that the Retailers were parties to the communications and NaviStone had their consent. (See Casper Compl. ¶¶ 16, 23.) However, without citing case law, Cohen alleges that, for "some of the communications at issue," the intended recipient of electronic communications was the internet service provider ("ISP"), rather than Defendants. (See Casper Compl. ¶ 48.) But ISPs are intermediaries who facilitate electronic communications, not recipients of such communications. See United States v. Ackerman, 831 F.3d 1292, 1294 (10th Cir. 2016) (explaining that an email never reached its

"intended recipient" because AOL, the ISP, had a filter which thwarted its transmission); United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010) ("An ISP is the intermediary that makes email communication possible. Emails must pass through an ISP's servers to reach their intended recipient. Thus, the ISP is the functional equivalent of a post office or a telephone company."); Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606, 613 (E.D. Pa. 2004) ("A hypothetical [electronic] communication . . . might originate on the user's computer, travel through . . . a regional ISP's network . . . and finally to the computer of the intended recipient of the communication."). NaviStone's assessment of this argument is spot on: "This is as farfetched as claiming that a cellphone call to L.L. Bean's customer service number was intended for AT&T alone." (NaviStone's Reply Mem. in Supp. of its Mot. to Dismiss, ECF No. 49, at 2.)

Thus, in an attempt to circumvent the consent rule, Cohen invokes 18 U.S.C. § 2511(2)(d)'s crime/tort exception, which states that consent diminishes liability "unless such communication is intercepted for the purpose of committing any criminal or tortious act." 18 U.S.C. § 2511(2)(d). This too fails because Defendants did not intercept communications "for the purpose" of committing a crime or tort.

In the Second Circuit, the crime/tort exception is "construed narrowly." United States v. Jiau, 734 F.3d 147, 152 (2d Cir. 2013). Under the exception, "for the purpose" means that the crime or tort was the "primary motivation" or "a determinative factor" behind defendant's conduct. In re DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 514–15 (S.D.N.Y. 2001); United States v. Tarantino, 617 F. App'x 62, 65 (2d Cir. 2015) (summary order). In analyzing the primary motivation of a recording, courts look to the purpose of the recording itself, not to the purpose of the underlying communications. See Jiau, 734 F.3d at 152. Therefore, the exception is "confined to instances where the recording party intends to use the

recording to harm or injure a recorded party, such as to blackmail, threaten, or publicly embarrass the recorded party." Jiau, 734 F.3d at 152; see also United States v. Jiau, 794 F. Supp. 2d 484, 487–88 (S.D.N.Y. 2011), aff'd, 734 F.3d 147 ("[T]he provision was not intended to suppress all recordings that were arguably made in furtherance of a crime . . . .").

Courts further hold that a tortious purpose must be intended at the time of the interception, such that the commission of a crime or tort alone does not create liability. See Caro v. Weintraub, 618 F.3d 94, 99–100 (2d Cir. 2010) ("There is a temporal thread that runs through the fabric of the statute and the case law. . . . If, at the moment he hits 'record,' the offender does not intend to use the recording for criminal or tortious purposes, there is no violation."). In addition, the intended tort must be "independent of the act of recording itself"—the tort cannot be the act of interception. Caro, 618 F.3d at 100.

Here, Cohen fails to allege that Defendants' primary motivation at the time of the alleged interception was to commit a tort. Instead, he claims that Defendants' purpose was to collect data, de-anonymize consumers, and disclose the de-anonymized data to other parties, and that these purposes amount to GBL violations. (See May 10, 2018 Oral Arg. Tr., Casper ECF No. 55 ("Tr."), 20:9–24.) That is not sufficient.

First, collecting data to de-anonymize consumers was not Defendants' primary motivation for installing the Code. Rather, it was the means Defendants used to achieve their real purpose—marketing. Cohen admits exactly that. (See Tr. 20:17–19 ("Because the defendants then disclose the de-anonymized data to other third parties to use for marketing purposes."); Casper Compl. ¶ 44 ("Casper does in fact share visitors' Personal Information with NaviStone for . . . marketing purposes.").) The Complaint further demonstrates the Code's true purpose, as Cohen alleges that "NaviStone has partnered with hundreds [of] e-commerce

websites," (Casper Compl. ¶ 1), to help these websites "unlock a new universe of 'ready to engage' customers," (Casper Compl. ¶ 19). Second, Cohen fails to demonstrate that Defendants' primary purpose was to commit a tort. Instead, he claims that Defendants' conduct amounted to a tort. (See Tr. 20:21–23 ("We allege one tortious purpose is to covertly de-anonymize the user which we say is a tort under GBL 349.") But whether a tort was committed is irrelevant—the test is whether Defendants intended to commit a tort. See Caro, 618 F.3d at 100. Cohen offers nothing to show that Defendants intended to violate the GBL.

Cohen's allegations are unsettling—"[w]ith just the click of a button, [Defendants] can access each [visitor's] deep repository of . . . information at practically no expense." Carpenter v. United States, No. 16-402, slip op. at 12–13 (2018). Such information may include names and IP addresses. But while disturbing, Cohen may not contort Defendants' surreptitious conduct into an illegal wiretap claim where consent bars such claims.

B. Section 2512 Claims

Cohen next raises a claim under 18 U.S.C. § 2512, another provision of the ECPA. Under § 2512, it is unlawful to possess devices specifically designed for wiretapping: "[A]ny person who intentionally . . . manufactures, assembles, possesses, or sells any electronic . . . device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of . . . electronic communications . . . shall be fined under this title or imprisoned not more than five years, or both." 18 U.S.C. § 2512(1)(b). But there is no private cause of action available under § 2512.

18 U.S.C. § 2520 states that any person whose electronic communications are intercepted may sue a defendant in a civil action. See 18 U.S.C. § 2520. It is an issue of first impression in this District whether Congress intended that provision to include violations of

§ 2512—though it is well established that it includes violations of § 2511. See DirecTV v. Meinecke, 2004 WL 1535578, at *2 n.2 (S.D.N.Y. July 9, 2004). But the weight of authority, including two courts within this Circuit, holds that there is no private cause of action. See DirecTV v. Deskin, 363 F. Supp. 2d 254, 260 (D. Conn. 2005); Meinecke, 2004 WL 1535578, at *2 n.2 (collecting cases from other districts holding no private cause of action); DirecTV, Inc. v. Lewis, 2004 WL 941805, at *6 (W.D.N.Y. Jan. 6, 2004).

Further, in DirecTV, Inc. v. Treworgy, the Eleventh Circuit provided a persuasive analysis regarding why no private cause of action exists. 373 F.3d 1124 (11th Cir. 2004). There, a satellite television broadcaster sued the owner of a pirate access device which intercepted satellite transmissions so the owner could avoid paying fees. Treworgy, 373 F.3d at 1125. The Eleventh Circuit held that a private cause of action did not exist because (1) a private cause of action would be "constitutionally problematic," in that plaintiffs who suffered no injury in fact would still be able to sue; (2) a plain reading of § 2520 excludes claims based on mere possession by plaintiffs; and (3) courts interpreting § 2520 before it was amended in 1986 held that there was no private cause of action, and nothing in the 1986 amendments expanded the class of violations giving rise to a civil suit. See Treworgy, 373 F.3d at 1127–29. This Court agrees and holds that there is no private cause of action under § 2512.

III. Stored Communications Act Claim

The SCA creates liability for anyone who "intentionally accesses without authorization a facility through which an electronic communication service is provided . . . and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such." 18 U.S.C. § 2701(a)(1). Cohen offers nothing more

than "labels and conclusions" that the communications were held in electronic storage. Iqbal, 556 U.S. at 678.

Under 18 U.S.C. § 2510(17), "electronic storage" means "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17). Cohen concedes that any electronic communications were "stored" on his personal device. (Pls.' Opp. at 2, 17 ("[T]hese files were placed on Plaintiff's computer . . . ."); Casper Compl. ¶ 32 ("NaviStone's wiretaps scan the visitor's computer for files . . . .").)

Judges in this District routinely hold that communications stored on personal devices are not held in electronic storage. See Obeid *ex rel.* Gemini Real Estate Advisors LLC v. La Mack, 2017 WL 1215753, at *9 (S.D.N.Y. Mar. 31, 2017) ("[T]he weight of authority regarding this aspect of the SCA holds that emails stored on an electronic communication service provider's systems after it has been delivered, as opposed to emails stored on a personal computer, are stored communications subject to the SCA."); Williams v. Rosenblatt Sec. Inc., 136 F. Supp. 3d 593, 607 (S.D.N.Y. 2015) ("Because communications downloaded to a user's computer terminal are neither stored on a temporary basis "incident to [their] electronic transmission" nor stored "by an electronic communication service for purposes of backup protection of such communication," the plaintiff's allegations . . . fail[] to state a claim."); Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 555 (S.D.N.Y. 2008); DoubleClick, 154 F. Supp. 2d at 511–12.

Rather, the SCA "is specifically targeted at communications temporarily stored by electronic communications services incident to their transmission—for example, when an email

service stores a message until the addressee downloads it." DoubleClick, 154 F. Supp. 2d at 511 (emphasis added). The "legislative history [of the SCA] reveals that Congress intended precisely this limited definition": "[A]ny temporary, intermediate storage . . . describes an e-mail message that is being held by a third party Internet service provider until it is requested to be read." DoubleClick, 154 F. Supp. 2d at 512. Further, Congress' statements when it passed the law dealt only with electronic communications services and made "no mention of individual users' computers." DoubleClick, 154 F. Supp. 2d at 512.

In DoubleClick, the court held that cookies, which are essentially files transferred from a web browser to a hard drive, were not held in electronic storage. See DoubleClick, 154 F. Supp. 2d at 512. "Indeed, if § 2510(17) were interpreted in the manner plaintiffs advocate, Web sites would commit federal felonies every time they accessed cookies on users' hard drives, regardless of whether those cookies contained any sensitive information." DoubleClick, 154 F. Supp. 2d at 512–13. That observation applies with equal force here, where the only electronic storage is alleged to be on personal computers or cell phones. (Compl. ¶¶ 2, 75.)

Finally, Cohen's reliance on Kaufman v. Nest Seekers, LLC, 2006 WL 2807177 (S.D.N.Y. Sept. 26, 2006), is misplaced. There, the plaintiff operated a website containing a "multiple listing forum for brokers to list and search for residential properties . . . and to manage their confidential client records, real estate listings, and advertisements," which defendant hacked into. Kaufman, 2006 WL 2807177, at *1–2. The website also offered email service. Kaufman, 2006 WL 2807177, at *4. The court held that plaintiff adequately alleged that its website—not a personal device—was akin to a facility through which an electronic communication service was provided because it served as an "electronic bulletin board" on

which users could post listings and access email service. Kaufman, 2006 WL 2807177, at *4–5. Cohen makes no such allegations.

IV. General Business Law Claims

Cohen brings claims under GBL §§ 349 and 350, which fall under New York's deceptive acts and practices laws. Defendants argue that (1) this Court should not exercise supplemental jurisdiction over these state-law claims; and (2) even if there is jurisdiction, Cohen fails to state a claim. Each argument is discussed in turn.

A. Jurisdiction

Under 28 U.S.C. § 1367(c)(3), this Court may decline to exercise supplemental jurisdiction where it has dismissed all claims over which it has original jurisdiction. However, this Court would still have original jurisdiction if the requirements of the Class Action Fairness Act ("CAFA") are satisfied. See 28 U.S.C. § 1332(d)(2). "To establish federal jurisdiction under CAFA, [plaintiffs] must prove to a reasonable probability that (1) there is minimal diversity (meaning at least one defendant and one member of the putative class are citizens of different states); (2) the putative class exceeds 100 people; and (3) the amount in controversy is greater than $5 million." Bigsby v. Barclays Capital Real Estate, Inc., 170 F. Supp. 3d 568, 579 (S.D.N.Y. 2016) (quotation marks and citations omitted).

There are several exceptions to CAFA which, if satisfied, destroy jurisdiction. See, e.g., 28 U.S.C. § 1332(d)(4). However, although the Second Circuit has yet to decide who bears the burden of establishing whether an exception exists, judges in this District have adopted "[t]he overwhelming weight of authority[, which] holds that Defendants, as the parties who seek to invoke [an] exception, bear the burden of proving by a preponderance that [an] exception applies." Simmons v. Ambit Energy Holdings, LLC, 2014 WL 5026252, at *3 (S.D.N.Y. Sept.

30, 2014); Anirudh v. CitiMortgage, Inc., 598 F. Supp. 2d 448, 451 (S.D.N.Y. 2009) ("Therefore, in the instant case, while plaintiffs bear the initial burden of establishing federal subject matter jurisdiction under CAFA, defendant bears the burden of proving that an exception to CAFA applies."). Here, Defendants fail to raise any exceptions, so this Court need not address them. See Wurtz v. Rawlings Co., LLC, 761 F.3d 232, 240 (2d Cir. 2014) ("Here, plaintiffs [seeking remand] have not claimed that any CAFA exceptions apply (or contested CAFA jurisdiction at all), so . . . these exceptions are not before us, and therefore we need not comment further."); Blockbuster, Inc. v. Galeno, 472 F.3d 53, 58 (2d Cir. 2006) (same).

Cohen adequately alleges minimal diversity and a putative class exceeding 100 people to a reasonable probability. (See Casper Compl. ¶¶ 5–6, 54.) The sufficiency of Cohen's allegations regarding the amount-in-controversy is a closer question because Cohen fails to allege damages specifically related to his GBL claims. However, "that is not fatal to [his] jurisdictional claim." Bigsby, 170 F. Supp. 3d at 579. "Where the pleadings themselves are inconclusive as to the amount in controversy . . . federal courts may look outside those pleadings to other evidence in the record." Orlander v. Staples, Inc., 2013 WL 5863544, at *2 (S.D.N.Y. Oct. 31, 2013). In so doing, this Court must construe all ambiguities and draw all inferences in Cohen's favor. See Aurecchione v. Schoolman Transp. Sys., Inc., 426 F.3d 635, 638 (2d Cir. 2005).

Cohen alleges that the nationwide class is "in the millions." (Casper Compl. ¶ 54.) GBL § 349(a) states that the alleged misconduct must occur in New York. Therefore, the GBL claims must relate to business Defendants conducted in New York. Moreover, GBL § 349(h) states that damages shall be equal to "actual damages or fifty dollars, whichever is greater," and that a court "may, in its discretion, increase the award of damages to an amount not

to exceed three times the actual damages up to one thousand dollars, if the court finds the defendant willfully or knowingly violated this section." As such, the minimum damages per violation would be $50. And Cohen alleges intentional violations and asks this Court to increase damages to three times the amount of actual damages. (See Casper Compl. ¶¶ 52, 81.) Therefore, to meet CAFA's amount-in-controversy requirement, even at the bare minimum damages level of $50, there would need to be 100,000 class members who could sue under the GBL. Given the population of New York State relative to the United States, and that Cohen alleges there are "millions" in the nationwide class, there is a reasonable probability that the amount in controversy exceeds $5 million. Therefore, this Court possesses original jurisdiction over the GBL claims under CAFA.

B. Merits

Jurisdiction aside, Cohen fails to state a claim. GBL § 349(a) provides that "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful." GBL § 350 states, "False advertising in the conduct of any business, trade or commerce or in the furnishing of any service in this state is hereby declared unlawful." These statutes share the same elements: "[A] plaintiff must allege that a defendant has engaged in (1) consumer-oriented conduct that is (2) materially misleading and that (3) plaintiff suffered injury as a result of the allegedly deceptive act or practice." Koch v. Acker, Merrall & Condit Co., 967 N.E.2d 452, 452 (N.Y. 2012) (quotations marks omitted). However, "GBL § 350 relates specifically to false advertising." Petrosino v. Stearn's Prods., Inc., 2018 WL 1614349, at *6 (S.D.N.Y. Mar. 30, 2018).

Use of the Code is consumer oriented because it has a "broader impact on consumers at large," in that it captures the electronic communications of every visitor to the

Retailers' website. Oswego Laborers' Local 214 Pension Fund v. Marine Midland Bank, N.A., 647 N.E.2d 741, 745 (N.Y. 1995). Whether it was materially misleading is more open to question. But even assuming the conduct was materially misleading, Cohen's inability to identify a cognizable injury is fatal. To allege a claim under the GBL, he must identify a "connection between the misrepresentation and any harm from, or failure of, the product." Small v. Lorillard Tobacco Co., Inc., 720 N.E.3d 892, 898 (N.Y. 1999). Here, the only alleged injury is a general invasion of privacy "through the exposure of personal and private information." (Casper Compl. ¶ 80; Moosejaw Compl. ¶ 69.) Cohen does not allege that any "expos[ed]" information was particularly sensitive or that it was "expos[ed]" for any reason other than marketing. (See Pls.' Opp. at 21.)

State court judges in New York have held that similar invasion-of-privacy allegations do not meet the GBL's injury requirement. See Amalfitano v. NBTY Inc., 9 N.Y.S.3d 352, 355 (N.Y. App. Div. 2015) (holding there was no injury where plaintiff alleged that his email address was taken); Smith v. Chase Manhattan Bank, USA, N.A., 741 N.Y.S.2d 100, 102 (N.Y. App. Div. 2002); cf. Manning v. Pioneer Sav. Bank, 56 Misc. 3d 790, 797 (N.Y. Sup. Ct. 2016) ("All that Plaintiffs have alleged is potential exposure of their personal information that has increased their risk of identity theft, not actual fraudulent charges. These allegations are too remote and not sufficient enough to confer standing on Plaintiffs as they do not constitute an injury in fact.").

The same holds true for judges in this District analyzing the GBL, including where invasions of privacy led to a user's being "spammed" (sent solicitations online). See Shostack v. Diller, 2016 WL 958687, at *5 (S.D.N.Y. Mar. 8, 2016) (holding that an "unquantifiable injury to a privacy interest" is not a cognizable injury under the GBL); Cherny v.

Emigrant Bank, 604 F. Supp. 2d 605, 609 (S.D.N.Y. 2009) (holding that being spammed is not a GBL injury). Thus, although Cohen's desire to maintain his privacy is well-founded amid recent "seismic shifts in digital technology,"[2] his allegations fail to overcome countervailing precedent. See Carpenter, slip op. at 15.

For instance, in Smith, the Second Department affirmed the dismissal of a GBL § 349 claim because a plaintiff did not adequately allege actual injury: "the 'harm' at the heart of this purported class action . . . is that class members were merely offered products and services which they were free to decline. This does not qualify as actual harm." Smith, 741 N.Y.S.2d at 102. Moreover, in Mount v. PulsePoint, Inc., the court held that allegations that "surreptitiously collecting [browsing history] information was a 'violation of [plaintiff's] statutorily protected privacy rights'" were inadequate. 2016 WL 5080131, at *11 (S.D.N.Y. Aug. 17, 2016). There, the court took issue with plaintiffs' failure to "identify any New York statute—or any New York state court decision—enshrining their right to privacy in anonymous (or perhaps pseudonymous) internet browsing history information." Mount, 2016 WL 5080131, at *11. Indeed, New York does not recognize a cause of action for invasion of privacy. See Farrow v. Allstate Ins. Co., 862 N.Y.S.2d 92, 93 (N.Y. App. Div. 2008) ("New York State does not recognize the common-law tort of invasion of privacy except to the extent it comes within Civil Rights Law §§ 50 and 51."). Moreover, the court confirmed that being spammed was not actual injury. Mount, 2016 WL 5080131, at *12. That holding was echoed in Cherny, where the court dismissed a § 349 claim because the only alleged harm was receiving spam. See Cherny,

[2] In fact, as the Supreme Court noted in Carpenter, "[t]here are [now] 396 million cell phone service accounts in the United States—for a Nation of 326 million people." Carpenter, slip op. at 1. And, "[u]nlike the nosy neighbor who keeps an eye on comings and goings," today's technology, including the Code here, is "ever alert and [its] memory is nearly infallible." Carpenter, slip op. at 15.

604 F. Supp. 2d at 609. Here, Cohen's claim cannot succeed where his only allegation is that his data was accessed.

Although the district judge in Mount cabined her holding to "anonymized" data, on appeal the Second Circuit noted that § 349's injury requirement can be satisfied only where "confidential, individually identifiable information—such as medical records or a Social Security number" has been collected. Mount v. PulsePoint, Inc., 684 F. App'x 32, 35 (2d Cir. 2017) (summary order). In fact, the district judge distinguished the New York state court decisions which held that invasion of privacy can be an injury under the GBL, because those courts "treated the information at issue as presumptively confidential." Mount, 2016 WL 5080131, at *12. Thus, like the plaintiff in Mount, Cohen "suppl[ies] no basis for us to assume that New York courts would consider the information allegedly collected here to possess a similar status." Mount, 2016 WL 5080131, at *12.

And this Court finds Mount's reasoning more persuasive than that in Bose v. Interclick, Inc., 2011 WL 4343517 (S.D.N.Y. Aug. 17, 2011)—the decision Cohen asks this Court to follow. In Bose, although the court held that collection of personal information, and thus invasion of privacy, constituted an injury under § 349, it merely relied on two New York Supreme Court cases in a one-paragraph explanation. Bose, 2011 WL 4343517, at *8–9. Those two cases are inapposite because they involved Social Security numbers and medical records, respectively. See Bose, 2011 WL 4343517, at *9; Meyerson v. Prime Realty Servs., LLC, 796 N.Y.S.2d 848, 850, 856 (N.Y. Sup. Ct. 2005); Anonymous v. CVS Corp., 728 N.Y.S.2d 333, 340 (N.Y. Sup. Ct. 2001). Further, these cases were considered in Mount, and the court concluded that "[t]he claimed injury [t]here d[id] not fit comfortably within th[e] precedent." Mount, 2016 WL 5080131, at *11–12. Cohen suffers the same fatal deficiency because his intercepted

information is akin to that in Smith, where defendants sold plaintiffs' "confidential financial information," resulting in products and services being offered to plaintiffs. Smith, 741 N.Y.S.2d at 102. There, the Second Department "did not focus on the disclosure of the customers' data as the central harm." Mount, 2016 WL 5080131, at *13.

Finally, because the elements of GBL § 349 are not met, Cohen's § 350 claim fails as well. Moreover, GBL § 350-a defines "false advertising" as "advertising, including labeling, of a commodity . . . ." Cohen offers one bare allegation against Casper and NaviStone related to false advertising: "Defendants engaged in . . . conduct . . . which constitutes false advertising." (Casper Compl. ¶ 83.) He failed to include this allegation in the Moosejaw and Tyrwhitt Complaints. Cohen cites no case law demonstrating that a privacy policy can constitute advertising, and this Court has found none. As such, the § 350 claim also fails because it does not relate to advertising.

CONCLUSION

For the foregoing reasons, Defendants' motions to dismiss the Complaints in these actions are granted. While Cohen alleges conduct raising troubling privacy concerns, that conduct does not violate any of the statutes on which Cohen predicates his claims. The Clerk of Court is directed to terminate all pending motions and to mark these cases as closed.

Dated: July 12, 2018
New York, New York

SO ORDERED:

WILLIAM H. PAULEY III
U.S.D.J.